

YAPAY ZEKÂ TEKNOLOJİLERİ VE VERİ KORUMA HUKUKU

Doç. Dr. Murat Volkan Dülger*

Yapay zekâ yazılımları ve bunlara bağlı çalışan sistemler, birer yazılım ya da cihaz olarak akıllı evler, akıllı şehirler, sanayi sektörü, sağlık, silahlı kuvvetler ve suç önleme gibi çeşitli alanlarda insanları zorlayan işleri başarmak ve çeşitli ihtiyaçları karşılamak için yeni ve değerli çözümler sunuyor. Tüm teknolojik gelişmelerde olduğu gibi, yapay zekâ teknolojilerindeki gelişmeler de bir yandan insanlığa büyük kolaylıklar sunarken diğer yandan temel hak ve özgürlükler açısından bazı ciddi riskleri de beraberinde getiriyor. Bilişim sistemlerinin giderek daha fazla veriyi işlemesi ve bunlardan anlamlı sonuçlar çıkararak karar alması üzerine kurulu olan yapay zekâ teknolojileri, kaçınılmaz olarak kişisel verilerin işlenmesini ve buna bağlı sorunları da gündeme getiriyor.

Yapay zekâ teknolojilerinin kişisel verilerin işlenmesindeki rolü ve veri koruma hukukunun ilke ve kuralları karşısındaki durumu aslında oldukça kapsamlı ve hassas bir incelemeyi gerektiren önemli bir konu. Bu çalışmada konuyu gerektirdiği ölçekte ele alamayacak olsam da kavramsal çerçeveyi belirlemeye ve yapay zekâ teknolojileriyle veri koruma hukuku ilişkisinin boyutlarını ortaya koymaya çalışacağım.

A. Konuya İlişkin Kavramlar

Yapay zekâ (artificial intelligence) ve bununla bağlantılı makine öğrenmesi (machine learning), nesnelerin interneti (internet of things) gibi kavramlar çoğunlukla yanlış ya da birbirinin yerine kullanılır¹. Kişisel verilerin korunması bağlamında konuyu doğru şekilde ele alabilmek için öncelikle ilgili kavramların netleştirilmesinde fayda görüyorum.

Yapay zekâ teknolojisi en genel tanımıyla, insan tarafından yerine getirildiğinde zekâ gerektiren görüntü algılama, konuşma tanıma, karar alma ya da diller arası çeviri yapma gibi görevlerin bilişim sistemleri tarafından yerine getirilmesini ifade eder². Daha teknik bir yaklaşımla yapay zekâ, çevresini algılayabilen ve herhangi bir hedef bakımından başarı şansını maksimize edebilecek şekilde karar alabilen zeki makineleri ifade eder³. Sonuç olarak yapay zekâ teknolojileri, dijital teknolojilerin verilerin çok hızlı bir şekilde kopyalanması ve işlenmesi gibi genel özelliklerini ve normalde insana özgü olan tecrübe gibi özellikleri bir arada bulundurulur.

Günümüzde gündelik hayatta sıklıkla karşılaştığımız strateji oyunları, sürücüsüz araçlar, çeviri programları, yüz tanıma sistemleri ve ticaret, sağlık ve araştırma alanında kullanılan istatistik programları aslında “dar anlamda” yapay zekâ teknolojileridir⁴. Gerçek anlamda yapay zekâ teknolojileri dar anlamda yapay zekanın yaptığı şablon tanıma ve tahmin etmenin çok ötesinde,

* Akademisyen / Avukat.

¹ CNIL, “Comment Permettre À L’homme De Garder La Main? Les enjeux éthiques des algorithmes et de l’intelligence artificielle”, 2017, s. 14.

² Türk Dil Kurumu’nun henüz kavrama ilişkin bir tanımı yoktur. Verilen tanım Oxford English Dictionary’den tercüme edilmiştir. https://en.oxforddictionaries.com/definition/artificial_intelligence.

³ Stuart J. Russell/Peter Norvig, Artificial Intelligence: A Modern Approach (3. ed.), Boston, Prentice Hall, 2010, s. 15, 30.

⁴ Lilian Mitrou, “Data Protection, Artificial Intelligence and Cognitive Services: Is The General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof?’”, Nisan 2019, s. 10.

tıpkı zeki bir insanın sınırsız değişkenlerle dolu bir çevrede geliştireceği bilişsel davranışlar ve görevler gibi öğrenebilen ve davranabilen teknolojilerdir⁵. Bu anlamda gerçek anlamda yapay zekanın belki de en önemli özelliği tahmin edilemezliktir.

Makine öğrenmesi (machine learning) kavramı, yapay zekâ ile aynı anlamda kullanılan ve aslında yapay zekâ teknolojilerinin ortaya çıkmasını sağlayan faktörlerden biridir⁶. Makine öğrenmesi yeni bilgi, şablon ve biçimler bulan ve veri hakkında etkili tahminlerde bulunmak için kullanılabilecek modeller oluşturan metodoloji ve teknikler serisini ifade eder⁷. Makine öğrenmesi program ve teknikleri önceden açıkça programlanmış olmaksızın gelişir ve tecrübe edinirler⁸. Yapay zekâ teknolojileri makine öğrenmesi teknikleri üzerine kuruludur⁹.

Yapay zekâ teknolojileri bağımsız ve izole bir alan olmayıp, bir takım özel gelişmeler ve trendlerle etkileşim içindedir. Yapay zekâ teknolojilerini destekleyen başlıca faktörler; devasa ölçekteki ve ucuz bilişim altyapısının mevcut ve erişilebilir olması, çeşitli alanlardan büyük veri setlerinin giderek daha da erişilebilir olması, giderek daha sofistike istatistik ve olasılık metodlarının geliştirilmesi, yapay zekâ ile yürüyen ya da yapay zekâ uyumlu alanların artması yönündeki eğilimdir. Bu itibarla yapay zekâ teknolojileriyle, özellikle veri işleme bağlamında son derece ilintili olan bir diğer kavram da büyük veridir (big data).

Bilişim ortamında her an çok fazla sayıda kullanıcı, sanal veya fiziksel cihaz tarafından inanılmaz büyük ölçekte veri işlenir. Bu veriler belirli süreçler bakımından yönetilebilir veya anlamlı olsalar da bunların bir yığın olarak veri setleri şeklinde bir araya gelmesi durumunda geleneksel işleme araçlarıyla yönetilemeyecek bir veri bütünü doğar. Bu ölçekteki düzenli ya da düzensiz veri setlerine büyük veri (big data) denir. Ancak yapay zekâ teknolojileri çeşitli ölçek, ebat ve formdaki büyük veriyle başa çıkabilir. Bu nedenle yapay zekâ ve büyük veri ayrılmaz kavramlardır¹⁰. Yapay zekâ teknolojileriyle büyük veri arasındaki ilişki çift yönlüdür: Bir yandan yapay zekanın kaynağını oluşturan makine öğrenmesi için geniş ölçekte veriye ihtiyaç duyulurken, diğer yandan da büyük veri setlerinden anlam çıkarabilmek için yapay zekâ teknolojilerine ihtiyaç duyulur¹¹.

Yapay zekâ teknolojisiyle birlikte teknolojinin evrildiği yönü işaret eden kavramlardan birisi de nesnelerin internetidir (Internet of Things). Nesnelerin interneti, çeşitli haberleşme protokolleri sayesinde birbirleri ile haberleşen ve birbirine bağlanarak, bilgi paylaşarak akıllı bir ağ oluşturmuş cihazlar sistemi olarak tanımlanabilir. Daha basit bir ifadeyle insan faktörü olmaksızın birbiriyle haberleşen bilişim cihazlarının oluşturduğu ağa nesnelerin interneti denmektedir. Giderek yaygınlaşan bu birbirine bağlı cihazlar ağı, yapay zekayla ayrılmaz bir ilişki içindedir. Büyük veri de olduğu gibi nesnelerin interneti ile yapay zekâ arasında da iki yönlü bir ilişki vardır: Nesnelerin

⁵ Mitrou, s. 11.

⁶ Mireille Hildebrandt, "Law as Information in the Era of Data-Driven Agency", The Modern Law Review, Vol. 79, 2016, s. 2.

⁷ Martijn van Otterlo, "A Machine Learning View on Profiling", Privacy, Due Process and the Computational Turn -Philosophers of Law Meet Philosophers of Technology, Eds: M. Hildebrandt/K. de Vries Abingdon, Routledge, 2013, s. 45.

⁸ van Otterlo, s. 46.

⁹ Mitrou, s. 13.

¹⁰ CNIL, "Comment Permettre À L'homme De Garder La Main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle", 2017, s. 18.

¹¹ Mitrou, s. 17.

interneti tam potansiyeline ulaşabilmek için yapay zekaya ihtiyaç duyarken, yapay zekanın hayatın her alanındaki varlığı nesnelerin interneti ile tamamlanmaya ihtiyaç duyar¹².

B. Yapay Zekâ ve Kişisel Verilerin İşlenmesi

Yapay zekâ teknolojilerine ilişkin süreçlerde oldukça büyük miktarda verinin (big data) işlenmesi söz konusudur. Burada kastedilen her türlü veri olmakla birlikte, kişisel veriler de kaçınılmaz bir şekilde yapay zekâ teknolojilerince işlenir. Tüm yapay zekâ teknolojileri kişisel bilgilerin işlenmesini gerektirmese de, makine öğrenmesi ve yapay zeka teknolojileri yazılımları kişisel verilerin işlenmesinde sayı ve değer bakımından oldukça çok ve geniş kullanım alanına sahiptir. Büyük veri ve makine öğrenmesi bağlamında gerçekleştirilen profillemeye manuel profillemenin çok ötesine ulaşmış ve yeni bir niteliksel ve niceliksel boyut kazanmıştır¹³. Makine öğrenmesi sayesinde büyük veriden anlamlı parçaların ve sonuçların çıkarılmasını ifade eden veri madenciliği kabiliyetleri artmıştır. Ekipman bakım kayıtları, kredi uygulamaları, finansal işlemler veya tıbbi kayıtlar içeren çok büyük kamusal veya ticari veri tabanlarından değerli bilgileri keşfetmek ve bunlara dayanarak öngörülerde ya da önerilerde bulunmak olanaklı hale gelmiştir.

Veri madenciliğinde kullanılan yapay zekâ teknolojileri, yapılarına ve amaçlarına bağlı olarak, gerçek kişiler hakkında çok fazla veriye ihtiyaç duyduklarından, onlar hakkında giderek daha fazla veri toplamaktadır. Kişisel veriler ve yapay zekâ iki yönlü bir ilişki içindedir: Bir yandan diğer tüm veriler gibi kişisel veriler de yapay zekâ teknolojilerini besler, karar alma süreçlerine malzeme oluşturma işlevi görür, diğer yandan yapay zekâ teknolojileri çıkarımlar yaparak daha fazla kişisel veri üretir¹⁴.

Gündelik hayatta sıklıkla karşılaştığımız bir arama motorunda aradığımız kelimelerle ilişkili, hatta bazen çok uzaktan ilişkili reklamların karşımıza çıkarılması, sosyal medya uygulamalarının tanyor olabileceğimiz kişileri ya da ilgimizi çekebilecek kişileri önermesi, internet ortamında maruz kaldığımız her türlü profillemeye, harita uygulamalarının trafiğin en uygun olduğu güzergahı önermesi, çeviri uygulamalarının zamanla sonuçları daha doğru hale getirmeleri, yapay zeka eliyle veri işlenmesinin en yaygın ve en anlaşılabilir örnekleridir.

Yapay zekâ teknolojileri kişisel veri koruma hukuku bağlamında birçok açıdan sorunsal oluşturur:

- Büyük veriye duyulan ihtiyaç bağlamında “tüm kişisel verilerin” veya “mümkün olduğunca fazla kişisel veri”nin toplanması,
- Mevcut verinin daha fazla öğrenmeye ve analize konu olarak veriden yeni veriler türetilmesi,
- Belirli bir bağlamda ve/veya işleme faaliyetiyle elde edilen verinin başlangıçta bilinmeyen ve çok çeşitli amaçlar için işlenebilmesi, yapay zekanın öngörülemezlik özelliği nedeniyle verinin işleme amaçlarının yeniden kurgulanmasının ya da amaçla sınırlılık ilkesine aykırı olacak şekilde çok fazla amaç için işlenmesinin önüne geçilememesi,

¹² Mitrou, s. 19.

¹³ Mitrou, s. 19.

¹⁴ Mitrou, s. 21.

- Giderek daha fazla otomatik karar alma mekanizmasına yer verilmesi.

C. Kişisel Veri Koruma Hukuku Uyarınca Yapay Zekâ İle Veri İşlenmesi

Yapay zekâ teknolojileri içerdikleri ve dahil oldukları veri işleme süreçlerinde kişilerin hak ve hürriyetlerini gözetmek, konumuz bağlamında kişisel verilerin korunması hakkını korumak ve kişisel verilerin korunması hukukuna uymak zorundadır. Yapay zekâ teknolojilerinin (henüz) kişiliği bulunmadığı için bu noktada yükümlülük ve sorumluluklar yapay zekâ teknolojilerini geliştiren, satan ve kullanan gerçek ya da tüzel kişiler bakımından gündeme gelecektir.

Kişisel veri koruma hukuku uyarınca yapay zekâ teknolojileri ile veri işlenmesi bağlamında yapay zekâ geliştiricileri, satıcıları ve kullanıcıları tarafından gözetilmesi gereken ilke ve kuralların belirlenmesinde Avrupa Konseyi 108 nolu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi Danışma Komitesi'nin konuya ilişkin rehberi yol gösterici niteliktedir. Buna göre¹⁵:

- Kişiler ve toplum açısından etki doğurabilecek yapay zekâ teknolojilerinin geliştirilmesi ve kullanılmasında temel insan hakları ve özellikle kişisel verilerin korunması hakkı esas alınır. Bu bağlamda özellikle karar alma süreçlerinde yapay zekanın kullanıldığı durumlar önemlidir.
- Kişisel verilerin işlenmesi süreçleriyle ilgili olan yapay zekâ teknolojilerinin geliştirilmesinde veri koruma hukukunun temel ilkeleri gözetilmelidir.
- Yapay zekâ alanında sorumlu yatırımlar yapılmalı, kişisel verilerin işlenmesine ilişkin risklerden kaçınmak ve bu riskleri gidermek temel yaklaşım olmalıdır.
- Veri işlemede risk (etki analizi) değerlendirmesi, yapay zekanın ve büyük verinin özellikleri gözetilerek daha hassas bir şekilde yapılmalıdır.
- Yapay zekâ teknolojileri ilgili kişilerin (KVKK m.11'de düzenlenen) haklarını gözeterek ve bu haklarını kullanabilmelerine imkân tanıyacak şekilde tasarlanmalıdır.
- Yapay zekâ geliştiren, satan ve kullananlar ilgili kişilerin yapay zekâ eliyle kişisel verilerinin işleneceği konusunda yeterli ve doğru bir şekilde bilgilendirilmesini ve şartları bulunduğu itiraz haklarını kullanabilmesini sağlamalıdır.
- Yapay zekâ eliyle işlenen veriler bakımından ilgili kişilerin verileri ve sürecin sonuçları üzerindeki kontrolü (hakimiyeti) sağlanmalıdır.
- Otomatik karar alma süreçlerine itiraz etme hakkı kapsamında yapay zekâ tarafından verilerin otomatik olarak işlenip, kişiler bakımından sonuç doğuracak kararlar alınması durumunda ilgili kişilere itiraz etme hakkı tanınmalıdır.
- Yapay zekâ geliştiren, satan ve kullananlar kişisel verilerin korunması alanındaki olası risklere karşı önleyici tedbirler almalıdır.
- Veri toplama dahil tüm işleme aşamalarında tasarım olarak verilerin korunması ilkesi (by-design) gözetilmeli, özellikle yapay zekanın ayrımcılık anlamına gelebilecek önyargılara sahip olmaması temin edilmelidir.

¹⁵ Guidelines on Artificial Intelligence and Data Protection, Consultative Committee of The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, T-PD(2019)01, Strasbourg, 25 January 2019.

- Tüm geliştiriciler işlenecek kişisel verilerin türünü, niteliğini, kaynağını ve miktarını değerlendirmeli gereksiz ve aşırı işleme faaliyetlerinin önü alınmalıdır. Bu bağlamda sentetik veriler (gerçek kişisel verileri modelleyen temsili veriler) etkili bir çözüm olabilir.
- Yapay zekanın veri işlemede bağlam dışına çıkması ve bu şekilde amaç dışı veri işlemesine ilişkin riskler saptanmalı ve gerekli algoritmik formüllerle önlenmelidir.
- Konu özelinde bağımsız danışma kurulları kurulmalı, mevcut kurullar ve akademik kurumlardan görüş ve öneri alınmalıdır.
- Risk değerlendirmede potansiyel ya da mevcut kullanıcı yorumlarını dikkate alan katılımcı yöntemler geliştirilmelidir.
- Yapay zekâ geliştiren, satan ve kullananlar, yapay zekanın veri işleminde her aşama ve süreçte hesap verebilir bir algoritma kurmalı ve sorumlulukların kime ait olacağını (veri sorumlusunun kim olacağı) kurgulamalıdır.